UCRL-WEB-201324

EZACCESS

Table of Contents

Preface

Scope: EZACCESS provides basic comparative information on the alternative paths by which users can reach Livermore Computing resources, the alternative techniques and tools (such as OTS, SSH, and VPN) available for using those access paths, and access administration help (such as password-policy summaries and password usage tips, pointers to authorization and identity-verification forms, and tips on finding additional basic user documentation relevant to computing at LC). A companion manual called the EZOUTPUT (URL: http://www.llnl.gov/LCdocs/ezoutput) guide provides similar basic comparative information about file transfers to and among LC machines. Technical instructions for dealing with LLNL's firewall and for using the more intricate access tools introduced here appear in a separate Firewall and SSH Guide. (URL: http://www.llnl.gov/LCdocs/firewall)

Availability: When the programs described here are limited by machine, those limits are included in their explanation. Otherwise, they run under any LC UNIX system.

Consultant: For help contact the LC customer service and support hotline at 925-422-4531 (open e-mail: lc-hotline@llnl.gov, SCF e-mail: lc-hotline@pop.llnl.gov).

Printing: The print file for this document can be found at

```
OCF: http://www.llnl.gov/LCdocs/ezaccess/ezaccess.pdf
SCF: https://lc.llnl.gov/LCdocs/ezaccess/ezaccess_scf.pdf
```

Introduction

EZACCESS is a basic user guide that describes alternative paths for reaching the Livermore Computing machines, alternative techniques and tools for taking advantage of those paths, and access administration fundamentals (such as the basic LC password policies and local usage techniques, along with authorization forms).

The goal of this guide is to help you solve access problems by either directly giving you the most relevant answers to the most common questions, or indirectly pointing to appropriate answers already in other places. LC has much access-relevant material scattered among many different web pages (and different web servers). EZACCESS therefore organizes (and sometimes summarizes) that material so that you can quickly decide which parts meet your needs and retrieve answers when you need them. EZACCESS also contains supplementary access-support information and comparisons not published elsewhere but needing a convenient home.

Several other LC user manuals address specific questions that newly arriving users often have:

- FIREWALL.
  Technical instructions for dealing with LLNL's firewall and for using secure shell SSH, local variant XSSH, and Virtual Private Network VPN appear in a separate manual called the Firewall and SSH Guide (URL: http://www.llnl.gov/LCdocs/firewall).
- STORAGE.
  Users concerned about accessing LLNL machines primarily to store project files or retrieve stored files should consult the EZSTORAGE (URL: http://www.llnl.gov/LCdocs/ezstorage) basic guide.
- LINUX.
  Users new to the Linux flavor of UNIX in general, or who want a careful comparison of Linux and AIX implementation features on LC production machines, can consult LC's Linux Differences (URL: http://www.llnl.gov/LCdocs/linux) user guide.
- ENVIRONMENT VARIABLES.
  Every UNIX computing system employes environment variables in its own peculiar way, and at LC many additions to the standard variable set help handle resources or job-control issues unique to LC's large clusters. For a comparative analysis of environment variables "in the wild" on LC machines, see the Environment Variables (URL: http://www.llnl.gov/LCdocs/ev) user manual.

Access Paths

This section compares the different access paths available (to different prospective LC users) and briefly explains the role and prerequisites for using each path.

Matrix of Alternatives

How you can reach LC machines depends on who you are, where you are located, and which machines (open or secure) you want to use. The left-hand column in the table below shows the who and where possiblities, while the X marks in the other columns reveal which paths are available to you based on your status and location. (The next section summarizes the key comparative properties of each access path listed here, to help you get started with the appropriate one.)

The table uses the following standard LLNL abbreviations for funding sources:

- ASC: Advanced Simulation and Computing Initiative (formerly Accelerated Strategic Computing Initiative).
- LDRD: Laboratory Directed Research and Development.
- M&IC: Multiprogrammatic and Institutional Computing.

Access Choices for LC Users, by Status and Location.

Status and Location	**SecureNet**	**Internet**	**OTS(*)**
LLNL Researcher			
On site:			
M&IC investors		X	X
M&IC ad hoc		X	X
LDRD proposals		X	X
ASC work	X	X	X
Off site:			
M&IC investors		X	X
ASC (at a DOE site)	X	X	X
Los Alamos or Sandia ASC Researcher	X	X	
Other DOE Sites	X	X	
ASC Strategic Alliance Users		X	

(*)OTS = Open Terminal Server (dial-up access).

Path Properties

SecureNet

ROLE:

SecureNet is a computer network designed to safely transmit classified information, up to and including Secret Restricted Data, exclusively among DOE sites. SecureNet has the following features:

- connects DOE sites only.
- connects secure (classified) computers only.
- uses gateway computers for enhanced security.
- supports SSH as access software.

PREREQUISITES:

To use SecureNet from LLNL to another DOE site you must be authorized by your professional collaborator at that site, whether it is another laboratory (LANL or SNL) or an industrial site (e.g., Pantex). Only a host (target) site can issue you a login and password to use SecureNet to reach that site. For a list of sites connected to SecureNet, including the machine types and domain names supported at each site, start at this URL:

```
http://www.llnl.gov/computing/securenet_info.html
```

INSTRUCTIONS:

LLNL's SecureNet home page, to which a tree of technical details about SecureNet use and support is connected, is now located at:

```
http://www.llnl.gov/computing/securenet_info.html
```

You can use SSH (secure shell) from another SecureNet site "inward" directly to a classified LLNL machine on which you have an LLNL account by supplying the full machine name, for example:

```
ssh um.llnl.gov
```

Details vary, however, depending on whether you have an account at LANL or SNL and want to "forward your credentials" to use an ASC LLNL machine, or if you want to use a non-ASC machine (that hence won't accept forwarded credentials), or if your user name differs at different SecureNet sites. For an explanatory matrix that shows how to handle these complex possibilities, see

```
http://www.llnl.gov/computing/hpc/access/remote_access.html
```

Internet

ROLE:

The Internet (off site) and Open LabNet (on site) are the default unclassified paths to and from all LC open machines, just as they are worldwide. (Note that in LLNL's SecureNet documentation, the Internet is always mysteriously called "the InterSite Network.") Thus ASC Strategic Alliance partners at nonDOE sites (such as universities and institutes) will routinely use the Internet to reach unclassified ASC machines located at LLNL. (In some publications and login greetings LC's unclassified computers were formerly called FAST, for "Facility for Advanced Scalable Computing Technology," a name replaced by OCF [for "Open Computing Facility"] in 1999.) The Internet has the following features:

- connects nonDOE sites with DOE sites.
- connects open (unclassified) computers only.
- supports TELNET and also SSH (secure shell) as access software.
  WARNING: Currently you can use TELNET among machines all of which are outside the llnl.gov domain and from inside llnl.gov to outside. But direct TELNET connections from outside LC's llnl.gov machines (from outside the 134.n.n.n IP address domain) to any LC machine within llnl.gov are now blocked by a firewall (a former TELNET gateway through the firewall, gw-lc.llnl.gov, was disabled in April, 2000). And TELNET use among LC's llnl.gov machines (among 134.n.n.n machines) themselves was also disabled in February, 2001. Only SSH connections from outside LC's llnl.gov machines and among those machines are still allowed. See the Login section (page 14) for a comparison of TELNET and SSH use; see below for SSH login tips.

PREREQUISITES:

You can become authorized to use LC's unclassifed computers (via the Internet) if you are either:

- an employee of a program that has invested in LC's hardware under the M&IC framework, or
- an LLNL scientist who has an approved ad hoc research proposal,
- an LDRD researcher, or
- officially collaborating with someone in the previous three categories, such as an ASC Strategic Alliance partner.

INSTRUCTIONS:

If you are eligible and want instructions on how to become authorized (i.e., on what forms to file), consult LC's "Guide for Offsite Users" web posting located at

`http://www.llnl.gov/computing/hpc/access/remote_access.html`

or consult the Forms (page 22) section later in this document. If you are already authorized and want instructions on how to reach various LC unclassified machines using SSH (such as the Linux-based MCR cluster), look for the specific login tables mixed with the classified instructions at the same URL (listed above).

BATCH:

Offsite, nonLLNL ASC collaborators can submit batch jobs through the Internet to run on the ASC UP IBM cluster or the ALC Linux cluster without logging on to it at all, if Globus job-management software

resides on their own (remote-to-LLNL) machine. There are many prerequisites. See the Globus User Guide (for LC) (URL: http://www.llnl.gov/LCdocs/globus) for an explanatory list of requirements, steps, and local modifications.

INTERACTIVE:

Using the Internet interactively to reach LC machines and services from offsite usually (with the few exceptions noted below) involves some combination of three special software tools:

- SSH.
  (1) The secure shell (SSH) is the only Internet *login* service from outside-the-firewall sites to LC machines that is allowed through the LLNL firewall (inward TELNET is not allowed). For a comparison of TELNET and SSH features, see the Login section (page 14) below.
  (2) SSH clients for Macintosh, Windows, and UNIX platforms are available to authorized LC users for free download from https://src.llnl.gov/software/ssh, as noted in the table below.
  (3) All offsite users must invoke SSH with port 922 to successfully connect to LC machines (use the -p 922 option, or set the port with the EDIT | PREFERENCES | CONNECTION chain of menus.
  (4) Starting in fall, 2005, all offsite users (except for SNL and LANL users who start from their own restricted ("yellow") network) must first run a VPN client to borrow an llnl.gov IP address before they can login to any LC machine. Timeouts apply; see details below. Only rare cases where no VPN client exists are still allowed to use IPA (see below).
  (5) Starting in September, 2005, LC machines only accept connections using the SSH version-2 protocol (which is the default protocol for all LC-provided SSH clients).

- IPA.
  IP Port Allow (IPA) is an interactive, web-based process for registering the IP address of an outside-the-firewall computer for a specified period (2 hours by default, see "TIMEOUTS" below) so that for that period the LLNL firewall allows SSH login service from that specific machine. WARNING: Only those very rare cases for whose offsite computer no VPN client exists are allowed to have an IPA account as of fall, 2005. Virtually everyone should see the VPN section below instead of following the IPA instructions here. If you are one of the few who have an IPA account already, follow these steps to authenticate an SSH session:
  (1) Use a web browser on your offsite machine to reach

  `https://access.llnl.gov/ipa/login`

  (note the s in https here).
  (2) Confirm the name of your computer and then enter your IPA official ID (which is your "official user name" OUN, your PH-reported LLNL e-mail ID, *not* your LC login name) and your IPA password (starting in June, 2005, this must be your authenticator-generated one-time password, OTP) in the form fields offered.
  (3) Click SUBMIT. A confirmation that your address is IPA registered will appear. You can then exit the web browser if you wish.
  (4) Run SSH (with port 922) to connect to your target LC machine; exit as usual when you are done with your interactive session. Starting in June, 2005, you can only use IPA to reach LLNL machines that themselves employ "two-factor authentication" (that is, an authenticator-generated one-time password, OTP, and a PIN). This *excludes* direct IPA access to the LITE (time accounting) and some e-mail servers at LLNL. But if you use SSH to first reach any LC OTP machine, you can then use LITE or one-factor e-mail from that intermediate machine indirectly.
  (5) After your SSH connection closes, once again reach https://access.llnl.gov/ipa/login with a web browser. Change ALLOW to REMOVE on the login page, enter your IPA ID (your OUN) and password again, and then click SUBMIT. This deactivates your IPA authentication.
  (6) See the "Timeouts" comments at the end of the VPN section below for warnings about both total-session and inactivity time limits for IPA connections.

- VPN.
  (1) Virtual Private Network (VPN) is a way to temporarily borrow an llnl.gov IP address (from a pool for that purpose), so that while a VPN client runs on your outside-the-firewall machine all other applications there (such as your web browser or your FTP client) perform with the same privileges that they would have if your computer were inside instead of outside the LLNL firewall.
  (2) Unlike IPA, VPN use requires that you download and install a VPN client on your machine and then execute it during every VPN authenticated session. Your VPN client interacts with one of two VPN servers (vpna.llnl.gov or vpnb.llnl.gov) at LLNL while it runs. VPN clients for Macintosh, Windows, and UNIX (Solaris and Linux) platforms are available to authorized LC users for free download from https://access.llnl.gov/vpn, as noted in the table below.
  (3) Only LLNL employees (and contractors) and certain other ASC collaborators can establish an authorized VPN account, whose ID and password (your authenticator-generated one-time password) are required to run the VPN client, by contacting the LC Hotline (paperwork and approvals are required).
  (4) For more details on getting, installing, and configuring a VPN client, see LC's Firewall and SSH Guide (URL: http://www.llnl.gov/LCdocs/firewall). Users who started VPN service before March, 2003, will need to change their VPN Client Profile file to reflect IP address changes for the VPN servers that were implemented at that time. Timeouts apply; see the next paragraph.
  (5) Users who installed a VPN client before October 31, 2005, must uninstall the old (VPN 5000) version and replace it with the newer (VPN 3000) client (available from the URL cited in (2) above). VPN 3000 instructions, including troubleshooting tips, are at https://access.llnl.gov/vpn/vpn3000-moreinfo.html (URL: https://access.llnl.gov/vpn/vpn3000-moreinfo.html).

TIMEOUTS:
Beginning in June, 2005, LLNL automatically disconnects *every* remote-access Internet (VPN or IPA, but not OTS) session if either--
(1) it remains *inactive* for 30 minutes, where "activity" includes incoming and outgoing traffic, e-mail checks, or web-page accesses (note that running jobs with reporting timesteps longer than 30 minutes could trigger this timeout), or
(2) 12 hours elapse since you last *authenticated* the session (only 2 hours for IPA). Reconnecting with VPN renews your 12-hour limit.

Your computing goals (tasks) and who you are jointly determine which mix of these three software tools (SSH, IPA, VPN), if any, you need to use to successfully interact over the Internet with LC machines. The alternatives are often complex, involve many tradeoffs, and may change as your goals and LC policy changes. (You can give yourself more flexibility in recovering from OTP login problems during remote access if you "enroll" in LC's optional identity-verification service in advance, as described in a later section. (page 28)) XSSH is a locally developed, high-efficiency alternative to standard SSH, but only available for use *among* LC machines (see the Firewall and SSH Guide (URL: http://www.llnl.gov/LCdocs/firewall)).

The table below summarizes the matrix of goals, personal status, and appropriate tools to help you make (and perhaps reevaluate later) the best access choices:

Goal or Task(+)	Personal Status	Access Tool(s) Needed
Reach public LLNL web sites. https://access.llnl.gov http://www.llnl.gov/computing	anyone	any web browser on any machine
Reach passworded web sites. https://access.llnl.gov/ipa/login https:/access.llnl.gov/vpn/login	authorized IPA or VPN user	any web browser on any machine
Reach LLNL-only web sites, or sites without one-time passwords (LITE, e-mail). https://src.llnl.gov/software/ssh	(1) authorized IPA user (very few) (2) authorized VPN user	(1) login to an LC machine with SSH, then run browser there (2) start VPN client locally, then use local browser
Login to LC machines.	(1) SNL or LANL user (2) authorized IPA (very few) or VPN user	(1) run SSH port 922 (2) authenticate at IPA page or start VPN, then run SSH port 922 (3) only SSH version-2 protocol supported
Transfer files to LC machines. (including to storage.llnl.gov)	(1) authorized IPA user (very few) (2) authorized VPN user	(1) authenticate at IPA web page, run SSH port 922, then use FTP/GET from LC (2) start VPN client locally, then use local FTP to PUT files to LC(*)

(+)Typical example sites are included here, but there are many others too.
(*)LC has confirmed that VPN enables inward file transfers with FTP when FTP and VPN run under Windows98, but you may encounter vendor-compatibility problems with other versions of Windows or with other operating systems.

See LC's Firewall and SSH Guide (URL: http://www.llnl.gov/LCdocs/firewall) for local implementation, installation, configuration, and usage details on the specialized tools introduced here.

Open Terminal Server (OTS)

ROLE:

For a $100 registration fee and a $200/year unlimited-usage fee, LLNL staff members with a valid cost account can arrange to use LLNL's Open Terminal Server for dial-up access to the open (unclassified) LC computers through telephone lines on site or off site. The Open Terminal Server (OTS) has the following features:

- 72 asynchronous serial ports with a maximum data rate of 115 kbits/s.
- 25 28,000-baud modems.
- several circuit-switched ISDN lines for transmission up to 19.2 kbaud (ATT DMI transport only, not V.120).
- support for Windows, MacOS, Solaris, and Linux remote systems.

PREREQUISITES:

Physically, you will need a "true V.34" protocol modem, such as the U.S. Robotics Courier modems used by OTS itself. To set up the modem, use 8 data bits, 1 stop bit, and no parity. Administratively, you will need:

- A valid LLNL cost (recharge) account number.
- A valid LLNL e-mail name and address.
- An LLNL-issued RSA authenticator (or "token"), a small plastic device that generates a new one-time password (OTP) (page 26) every 30 seconds (required for OTS as of February 18, 2003). To get an OTP authenticator or to change the PIN for one, contact the OTS open web site at (note the s in https):

  `https://access.llnl.gov/ots`

INSTRUCTIONS:

To arrange for OTS use (to "register"), have your cost account number and your e-mail ID handy, and then contact your OISSO (Organizational Information System Security Officer) or their authorized designee. If you don't know who is your OISSO, consult the OTP support page at (note the s in https):

`https://access.llnl.gov/oisso.html`

Also available from this web page is a downloadable PDF file that you can print to make a copy of the OTS "Access Account Sign-Up Form," needed for your OISSO's approval of your proposed OTS account. For OTS help or advice from offsite, send e-mail to

`Access-Help@llnl.gov`

To read more detailed instructions for OTS use, including specific tips about ARA, PPP, SLIP, and LAT service, consult Open LabNet's hypertext user manual located at:

`https://access.llnl.gov/ots_access/index.html`

POST-CONNECT AUTHENTICATION:

Orignally, you provided your login name and (one-time) password (OTP) *before* your computer's modem and the OTS modem negotiated a connection. Experience showed this process to be so variable in length that the time-sensitive OTP often expired before OTS could establish a successful link. (Clock drift in OPT authenticator "tokens" made this problem worse.) Therefore, starting in February, 2005, OTS switched configuration to request your login name and OTP only *after* the dialing/modem negotiation has completed. Such "post-connect authentication" or "post-authentication" largely eliminates the stale-password problem and improves connection reliability. If you have already configured your Windows XP or Windows 2000 offsite computer for pre-connect authentication, however, you must reconfigure it for post-connect authentication to work successfully with OTS now. Follow the instructions at the appropriate URL (note the 's' in https):

https://access.llnl.gov/ots_access/ots-winxp-newconnect.html
https://access.llnl.gov/ots_access/ots-win2k-newconnect.html

USE:

After you have registered for OTS service and set up your modem properly, you can dial up OTS for a connection to LC machines by using one of these telephone numbers:

```
Local:           925-423-9330
Long distance: 1-800-827-7875 (US only)
Long distance: 1-877-284-4645 (US and Canada)
ISDN (on site):  925-423-8080
```

NOTE: regular telecommuters should get a departmental LLNL calling card and avoid the 800 service, which does accrue per-minute costs to the laboratory (intended for travelers only). The 2-hour timeout for Internet remote-access sessions does not apply to OTS.

Access Techniques

Login: SSH Replaces TELNET

LC supports one primary software tool for network access to LC production machines: SSH (the "secure shell"). SSH provides strong authentication and protected communication even over unsecure networks, but it demands considerable customization to use.

FORMER CHOICES.
The TELNET login utility is more familiar than SSH to most Internet users. TELNET clients are almost universal, but this tool does not protect your network traffic from third-party monitoring. So LC disabled all TELNET access to and among its machines in February, 2001 (outbound TELNET to other domains remains available). RLOGIN, used for remote logins in some UNIX environments, is no longer supported on LC machines because of its security vulnerabilities. SSH really takes the place of RLOGIN in focus and interaction style.

COMPARISON TABLE.
This table compares the main features of TELNET (disabled except for outbound) and SSH (along with secure copy SCP) as tools to interact with remote machines:

	TELNET	**SSH**
Execute line(s):	telnet *[targethost]* ...open *[targethost]* ...close ...quit	ssh -p 922 *targethost* ssh -p 922 *thost command* ssh -p 922 *thost* xterm scp *host1:fl1 host2:fl2*
Interaction style:	By session	By session or single remote command
Security:	No exchanges encrypted, Prompts for unencrypted password	All exchanges encrypted, Password encrypted or avoided
Prerequisites:	(1) universally available, (2) no personal setup needed	(1) target must have SSH daemon, (2) needs setup on both client and target hosts, (3) no world or group W access allowed on target home directory
Firewall effect:	Blocked except outbound	Allowed in both directions from any Internet host
SCF role:	Blocked (except SecureNet)	Allowed in both directions from any secure host

The "firewall" row in this table points out a difference between TELNET and SSH that is very important if you plan to connect to a machine within LC's portion of the llnl.gov domain (the machines sharing the 134.n.n.n IP address) from any machine outside that domain. LC has enabled a firewall that blocks all TELNET traffic originating from nonLC machines (from all machines outside 134.n.n.n, even from other

llnl.gov machines), although it freely allows SSH traffic originating from those machines. TELNET connections among LC machines themselves are also disabled (starting in February, 2001). So now offsite and even onsite users must install and run SSH to reach or connect between any LC machines. For details on how LC's firewall affects inbound TELNET sessions, or for instructions on getting and initializing SSH service, consult the Firewall and SSH Guide (URL: http://www.llnl.gov/LCdocs/firewall).

TELNET (for use from LC machines only "outward" to other Internet hosts, such as to UC's melvyl.ucop.edu) is simple enough to require little instruction or troubleshooting, and standard UNIX texts usually summarize its features.

SSH TIPS.

On the other hand, you will definitely need detailed local instructions to start using SSH. Furthermore, these instructions vary depending on your LC target host (e.g., common home directories make a difference) and on whether you work in the open or SCF environments. A concise but thorough SSH overview, including role, annotated setup steps, basic execute lines, and troubleshooting tips, is available in the second half of LC's Firewall and SSH Guide (URL: http://www.llnl.gov/LCdocs/firewall). This manual is posted on both the open and secure LC documentation web servers. There is also a MAN page for SSH and SCP on each LC machine that supports these programs (see also the summary in the Internet section (page 7) above). One section of the Firewall and SSH Guide explains how to use XSSH, a locally developed low-overhead variant of SSH that can significantly improve performance during graphics-intensive sessions *among* LC production machines. Another section explains how to enable local display of output from X-Windows programs that run remotely on LC machines (called SSH X11 forwarding). Note that (1) all Internet remote-access sessions connecting from external machines to LLNL machines now have a 2-hour timeout (page 7), and (2) only the SSH version-2 protocol is supported on LC machines.

The SCF row in the table above points out that similar restrictions apply to TELNET use even on LLNL's classified network. The classified network has always been physically isolated from the Internet. But in June, 1999, LC also began blocking all TELNET traffic originating from nonLC classified machines (from machines outside 130.n.n.n). In February, 2001, TELNET traffic among LC's classified machines themselves was blocked. Only incoming SecureNet (page 6) connections, which go through a gateway (proxy server) before reaching OAK (now just an alias for SC39) or ALDER (now just an alias for SC40), are still allowed to use TELNET service. As on the open network, SSH traffic is freely allowed in both directions between LC and nonLC classified machines. For the convenience of classified-network users who need SSH because of these restrictions on TELNET, site-licensed SSH software is available in /usr/local/bin on all SC-cluster machines.

File Transfer: FTP, NFT, or SCP

Transferring files between machines is a common need and LC's EZOUTPUT (URL: http://www.llnl.gov/LCdocs/ezoutput) guide addresses this need in thorough, systematic, but basic terms, complete with instructions and annotated examples. This section does not attempt to summarize everything in EZOUTPUT. Rather it alerts you to the primary file-transfer issues and tools important for practical success in LC's computing environment.

FTP: General File Transfers.

FTP is the most well-known and generally supported file-transfer utility, and so FTP clients and (server) daemons are available on all LC production and special-purpose machines in both the open and secure environments. With two exceptions, personal passwords are required when you use FTP (see the Passwords (page 23) section for which ones):

(1) STORAGE. FTP is also the standard interface to the LC archival file-storage system (both open and secure). But when you run FTP (on an OTP- or DCE-passworded LC machine) with STORAGE as the target host, access is "preauthenticated" and you are NOT prompted for your password.

(2) ANONYMOUS FTP. LLNL maintains an institutional anonymous FTP server in the open environment (ftp.llnl.gov) only. This server can sometimes greatly simplify transferring files to or from distant colleagues, especially nontext files where FTP's binary mode is desirable. Here you use ANONYMOUS as your username and your e-mail address as only a dummy password. For details, see EZOUTPUT (URL: http://www.llnl.gov/LCdocs/ezoutput).

Firewall alert: LC now uses its firewall to block direct FTP connections from machines outside the llnl.gov domain to LC machines within llnl.gov. Offsite users must now FTP outward after logging on to an LC machine (or LLNL badgeholders can arrange to use inward FTP after first executing a Virtual Private Network VPN client on their outside machine). LC's former FTP gateway has been disabled. See the Firewall and SSH Guide (URL: http://www.llnl.gov/LCdocs/firewall) for detailed instructions on installing and using VPN to enable inward FTP for authorized users.

NFT: Locally Enhanced Transfers.

Available on all LC production machines (open and secure, but not on some special-purpose hosts) is a locally developed file transfer tool called NFT. Although NFT uses standard FTP daemons to carry out its file transfers, it offers such enhanced features as transfer between two remote machines without being logged in to either one, "persistent" transfer even if the receiving machine has temporary problems, and preauthenticated (passwordless) file transfer. NFT's default settings also facilitate reliably transferring files to or from archival storage. Basic NFT instructions appear in EZOUTPUT (URL: http://www.llnl.gov/LCdocs/ezoutput), while the NFT Reference Manual (URL: http://www.llnl.gov/LCdocs/nft) gives complete details.

SCP: Encrypted File Transfers.

Available on those machines where the secure shell (SSH) has been installed and enabled for you is a secure (encrypted) version of the remote copy (RCP) utility called SCP. SCP is not limited to just LC's own "secure network," and indeed it improves file-transfer safety most when used to transfer files on the open Internet. SCP is sessionless (no overt log-in to the remote machine), but it does demand your one-time password for authentication. Unlike FTP, you cannot use SCP to store files or to contact the "file interchange service" (FIS, below), in either the open or secure environments at LC. For comparative execution details with FTP and NFT, see EZOUTPUT (URL: http://www.llnl.gov/LCdocs/ezoutput).

FIS: Open-Secure Transfers.

FIS is LC's open-to-secure (and secure-to-open) "file interchange service." LC's open and secure networks are physically isolated from each other, but you can transfer files between them by using FTP and two specially designated transfer nodes. You FTP the file(s) to the outbound directory of one network's transfer node, an LC operator moves the file(s) on tape between networks, and you retrieve them (with FTP) from the inbound directory of the other network's transfer node. Authorized Derivative Classifier review of all secure-to-open file transfers is required (as is use of your open and secure one-time or DCE passwords), and you cannot use NFT or SCP. For the necessary administrative as well as technical instructions, see EZOUTPUT (URL: http://www.llnl.gov/LCdocs/ezoutput) or consult the FIS Reference Manual (URL: http://www.llnl.gov/LCdocs/fis).

Common Home Directory "Transfers."

On most LC machines your UNIX home directory is not local, but NFS mounted to several machines at the same time (hence it is a shared or "common home" directory). Placing a file in the common home directory eliminates the need to overtly transfer it between machines using FTP or NFT, because it automatically appears to reside on all the machines that share that directory. Disk-space quotas and NFS side effects apply. Basic advice on using common home directories appears in the EZFILES (URL: http://www.llnl.gov/LCdocs/ezfiles) guide, while the full analysis of their benefits and limits is in the Common Home Reference Manual (URL: http://www.llnl.gov/LCdocs/chome). Never perform massively parallel I/O to your common home directory (it slows traffic for users on *all* machines.)

HTAR: Transferring TAR Files Efficiently.

HTAR is a locally developed, special-purpose transfer tool that efficiently moves files into or out of TAR-format archives (library files) either in the OCF or SCF storage systems or on other LC hosts, even when the files or archives are very large. See the HTAR Reference Manual (URL: http://www.llnl.gov/LCdocs/htar) for a thorough discussion of HTAR's helpful but very specialized file-transfer role.

X Terminal Control: XHOST or XAUTH

For an X client (such as the TotalView debugger) to display on an X-display server (such as your X terminal or workstation), the client must be authorized to connect to the server. XHOST and XAUTH offer alternative ways to manage this authorization.

Many users run the XHOST utility on the server machine to authorize X clients running on a specified host to connect to the server. This method is called host-based access control. It poses inherent security problems: any user on the specified host can access your display, and indeed any user can capture all your keystrokes too. Running

```
xhost +mcr39.llnl.gov
```

for example, authorizes several hundred users on MCR39 to connect to your server. The reverse is also true: running

```
xhost -mcr39.llnl.gov
```

prevents every user on MCR39 from connecting to your X server, including yourself.

LC recommends that you use a user-based, rather than a host-based, access control method. User-based access control avoids most of the security deficiencies present with host-based access control. The most common user-based access control method is called MIT-MAGIC-COOKIE-1. The basic idea is that a code (a long hexadecimal number) called a magic cookie is supplied to your X server, where it is kept in a file called .Xauthority in your server's home directory (on your workstation or X terminal). For an X client running on a remote host to connect to your display server, the same magic cookie must be (previously) placed in the .Xauthority file in your home directory on the remote machine. Then when you start an X client on the remote machine, the magic cookie in its .Xauthority file is passed to your display server. If the two magic cookies match, authorization is granted. The .Xauthority files need only be set up once.

This method of user-based access control requires two steps. First, the .Xauthority file in your server's home directory must be set up and supplied with the magic cookie. Second, the .Xauthority file in the remote machine's home directory must be established and given the same cookie. Fortunately, many LC production computers share common home directories. This gives you the convenience of setting up just one .Xauthority file in your common home directory that allows you to open windows on your display from clients running on any of the remote hosts that share that directory.

XAUTH is basically a utility program that manipulates such .Xauthority files (examples follow). Running XAUTH with no options returns an xauth> prompt. You can respond with a question mark to see a list of XAUTH commands, or type

```
help command
```

to get information on a specific command.

WARNING: host-based access control (with XHOST) overrides user-based access control (with XAUTH). If you have used XHOST to declare a whole host's access to your X server, then all users on that host can access your server even if you also implement magic cookies by running XAUTH.

Setting Up Server Authorization

The X-window system is started up using either XDM (X display manager) or XINIT. Which program your system uses deterimines how much work, if any, you need to do to set up user-based authorization on your server machine.

If you are using XDM (for example, under the Common Desktop Environment CDE), the X server is always running and you start your individual X session by logging in via a dialog box. User-based access control is built into the XDM control protocol. This means that the .Xauthority file will automatically be set up for you and the magic cookie told to your server when you log in. You can skip to the next section.

If you are using XINIT, you may have to set up authorization on the server machine yourself. Some window managers, such as OpenWindows, do this for you. If you have a .Xauthority file in your home directory on the server machine, then authorization was probably set up for you. If your home directory lacks a .Xauthority file, you can create one using XAUTH. First, you must create a pseudorandom number to be used as the magic cookie code. This should consist of an even number of hexadecimal digits. One method of generating a suitable magic cookie is with:

```
cookie='echo "(obase=16;$$^3)" | bc'     [Korn/Bourne shell]
set cookie='echo "(obase=16;$$^3)" | bc' [C shell]
```

You can add this magic cookie to the .Xauthority file by running XAUTH twice:

```
xauth add $(HOST)/unix:0 . $cookie
xauth add $(HOST):0 . $cookie
```

Then you must start the X server using this code, which can be done by running XINIT with a special argument:

```
xinit -auth $HOME/.Xauthority
```

Setting Up Client Authorization

After setting up server authorization (previous section), you must set up the corresponding .Xauthority file on each remote machine where you will be running X clients. First, use XAUTH on your server (here xyz.llnl.gov) to list the contents of your .Xauthority server file, extract the magic cookie code, and place it in a new file (here called AUTHFILE) for exporting to remote client machines:

```
xauth list
      xyz.llnl.gov:0 MIT-MAGIC-COOKIE-1
          e471b4f5a9ed8674fe38bcd2b01f8ab9
      xyz/unix:0 MIT-MAGIC-COOKIE-1
          e471b4f5a9ed8674fe38bcd2b01f8ab9
xauth extract authfile xyz.llnl.gov:0
```

Next, move AUTHFILE to the remote machine(s) and place it in your home directory (using FTP). If a .Xauthority file does not already exist there, you can just rename (MV) your AUTHFILE to .Xauthority. If .Xauthority already exists, merge the two files by running XAUTH on the remote machine:

```
xauth merge authfile
```

If for some reason you cannot FTP your extracted cookie file (here AUTHFILE) to the remote machine, you can run XAUTH on the remote machine and add the cookie by hand using an execute line of this form (obviously error prone unless you cut and paste the cookie string):

```
xauth add xyz.llnl.gov:0 e471b4f5a9ed8674fe38bcd2b01f8ab9
```

Your X clients on the remote machine can now authorize themselves to display on your X server (here xyz.llnl.gov).

Remember too that many LC production computers share common home directories. Setting up one .Xauthority file in your common home directory allows you to open windows on your display from clients running on any of the remote hosts that share that directory, without further use of XAUTH.

Avoiding Clear Passwords with MacX

Starting in the fall of 1999 LC is disabling all REXEC requests originating from outside the LC network (outside llnl.gov). REXEC is the means by which Common Desktop Environment (CDE) applications such as MacX and eXodus transmit passwords in clear text to LC hosts. So if you wish to use MacX (or other CDE applications) from outside the LC network, you must now follow these steps to transmit your encrypted password yet allow unencrypted (and hence much faster) regular X data exchange:

(1) Launch MacX (or other CDE application) but do NOT use any alias or shortcut (technically, any XDMCP or X Display Manager Control Protocol session) that brings up the usual CDE "desktop" for login.

(2) Launch SSH.

(3) Open an SSH window to your desired LC target machine (e.g., GPS01) by supplying your usual login name and one-time password (OTP) in the dialog box that SSH offers.

(4) On the LC target machine (e.g., on GPS01), set the DISPLAY environment variable to the IP address of the personal computer where you are running MacX. For example, using the C shell and the Macintosh 134.9.12.48, you would type (note the uppercase)

```
setenv DISPLAY 134.9.12.48:0
```

You can discover your Mac's current IP address, which might change with each Internet Service Provider session, by checking the Apple Menu | Control Panels | TCP/IP panel.

(5) On the LC target machine (e.g., GPS01), execute XTERM in the SSH window. This creates another window (labeled "xterm") in which you can run the X applications (such as the debugger) you desire. You will never see the standard CDE login dialog box if you follow these steps. Note, however, that under Mac OS X version 10.4 (called "Tiger"), display of remote X-application output on your Mac screen using an SSH connection is *disabled* by default. See the "Macintosh X11 Forwarding with SSH" section (URL: http://www.llnl.gov/LCdocs/firewall/index.jsp?show=s4.2.6) of LC's Firewall and SSH Guide for three ways to enable it.

Numerical Node Names at LC

Some LC machines or cluster nodes have all-character names (the LUCY or RAMON special-purpose Suns, for example). But often the number of names needed calls for using digits instead of just characters (e.g., MCR1024). Numerically naming the nodes of a massively parallel computer (or of a many-noded cluster) poses subtle problems, however, if not handled with a consistent, foresighted policy regarding:

- The start digit (0 or 1?),
- The use of leading zeros (is a single-digit node called 3 or 03?), and
- The numerical range of available nodes (is it 0 to 31, or 1 to 32?).

At LC, all such node-naming decisions have been ad hoc, so that even machines with the same hardware or the same operating system (Linux) may have different node-naming schemes. Hence, numerical node names here vary in regard to all three features above, and this chart summarizes the mixed empirical results:

Machine or Cluster	**Start Digit?**	**Leading Zeros?**	**Name Range?**
SC	1	no	sc1 to sc8
all IBM AIX	001	yes	up001 to up108, um001 to um128, etc., tempest01 to tempest12
GPS Cluster	01	yes	gps01 to gps32, gps320 (gps15-gps19 interactive)
MCR Linux Cluster	1	no	mcr1 to mcr1152
Intel Linux Cluster (ILX)	1	no	ilx1 (eye-ell-eks 1) to ilx67
ACE Linux Cluster	1	no	ace1 to ace176
ALC	1	no	alc1 to alc960
Lilac Linux Cluster	0	no	lilac0 to lilac767
Thunder Linux Cluster	0	no	thunder0 to thunder1023
BlueGene/L	1	no	bgl1 to bgl65536

For interactive log on, some LC machines with leading-zero node names use a single generic name (up, uv, um) that automatically assigns you randomly to one of the available log-on nodes (without your having to specify the leading zeros). Other clusters (GPS) accept log-on requests without leading zeros (gps1) and assign you automatically to the corresponding node with the leading zeros supplied (gps01); but note that *high* number GPS nodes gps15 through gps19 are the ones intended for interactive use.

Access Administration

Forms

At LC, every significant administrative change (new users, new user groups, new privileges, new FIS access) requires a paper form. And these forms require appropriate, original authorizing signatures (usually division-leader level) along with the usual identifying information. Send or deliver completed forms requesting new or changed computing service to:

```
LC Hotline
B-453, L-63
LLNL, P. O. Box 808
Livermore, CA 94551
```

LC administrative forms are available in three ways:

(1) From the LC Hotline.
Since which form to use or how to correctly complete the form is sometimes less than obvious, visiting the Hotline office or calling the Hotline staff (925-422-4531) to discuss your administrative needs often proves the most practical approach to handling LC forms.

(2) Open web access.
In the open environment (from any Internet host, including those off site), you can use any WWW browser to contact the URL:

`https://www.llnl.gov/lcforms`

This site lists and briefly describes over two dozen often-needed LC forms, including OCF, SCF, Foreign National, and FIS forms. Every entry here links to the corresponding form. These forms are quasi-interactive: you can complete the fields by supplying input from your terminal, but you CANNOT submit the completed form electronically. You must print the (completed) form, get the necessary signatures on the paper copy, and then mail or deliver the form to the LC Hotline for processing.

(3) Secure (SCF) web access.
In the secure LC environment, you can use any WWW browser to contact the SCF URL

`https://lc.llnl.gov/lcforms`

This site lists and describes the same LC administrative forms as the OCF URL above, with DCE forms added. Every entry in the SCF forms list is an online link to the corresponding form. Again, you can complete most forms online, but you must print them to get needed signatures and deliver the form to the LC Hotline.

Passwords

For historical reasons, LC machines have used a variety of passwords and authentication techniques (Kerberos, Distributed Computing Environment [DCE], unique, and most recently, one-time or "OTP"). Virtually all have been replaced by the DCE or OTP approaches, in response to Y2K concerns and a desire for enhanced security. Nevertheless, open and secure passwords are never the same, even when the authentication mechanism is the same. So if you use a variety of LC machines, password management still requires some careful attention.

Password Map

These two tables show for each machine (type) in open and secure environments the password scheme that applies to it (now largely standardized on DCE or OTP).

Open machines	Password scheme
Compaq GPS cluster	Open OTP
Open Linux clusters	Open OTP
Open STORAGE	Open OTP (first use only)
Open FIS node	Open OTP
Sun LUCY	Open OTP

Secure machines	Password scheme
Compaq SC cluster	SCF DCE or OTP
IBM AIX machines	SCF DCE or OTP
Secure STORAGE	SCF DCE or OTP (first use only)
Secure FIS node	SCF DCE or OTP
POP (mail) server	SCF DCE or OTP
SCF web pages	SCF DCE or OTP
SCF Linux clusters	SCF DCE or OTP

DCE Techniques

(1) Normal login. When you log in to an LC machine that uses DCE passwords (this includes all LC production machines), you are prompted for your user name and then your password. You are allowed five (5) iterative attempts to provide the correct password. If your fifth try is still incorrect, your access to the machine is locked, and you must contact the LC Hotline by calling 925-422-4531 to have the lock released. Locked access will NOT release simply by waiting.

(2) Voluntary change (SCF). To voluntarily change a working DCE password (e.g., because others might have inadvertently learned it) in the SCF environment:
(A) Start on any machine that offers a World Wide Web browser (client) and go to the URL

```
SCF:  https://lc.llnl.gov/bin/passwd
```

(note this involves https rather than http).
(B) Each DCE password-change web site will respond with a dialog box that says

```
Enter username for IntraVerse [/.../spectrum.llnl.gov]...
```

Supply your relevant login name and your current, working DCE password in the text-entry fields and click on OK.
(C) The web site will then ask

```
What kind of password would you like?
     o Random characters.
     o Nonsense syllables.
     o Pronounceable nonsense.
```

(A fourth former choice, "real words," was suspended in June, 2000.) You can click on one of the offered radio buttons to change the format of the password choices you will receive.
(D) Click the START button to see 25 computer-generated DCE password choices displayed in groups of 5. All 25 remain valid choices (if you can remember them), but you cannot page back to see previous groups again. To see the next group of 5, use the GET MORE CHOICES button.
(E) To change to one of the new (offered) passwords, you must insert your current DCE password in one text-entry field and your chosen replacement password in another field, then use the CHANGE MY PASSWORD button.
(F) To move to another set of 25 computer-generated password choices, leave all text-entry fields empty and use the START OVER button.
(G) To leave your current, working DCE password in effect, UNchanged, just avoid all buttons and fields on this web site and (at any time) use the browser's FILE menu to open a different URL (or exit the browser).

(3) Expired password. Within one month of your DCE password's pending expiration, you will be warned whenever you log in to a DCE-authenticated machine that you must get a new password by following step (2) above. After your DCE password has already expired, however, you cannot log in even once to get yourself a new password interactively. After expiration, your only recourse is to go to the LC Hotline office (B-453, first floor) and have a staff member reset your password with your help. New passwords CANNOT be "delivered" by telephone or e-mail.

Kerberos Techniques

Kerberos techniques are obsolete on all public LC machines.

(1) Normal login. No public machines on either OCF or SCF still use Kerberos passwords.

(2) Voluntary change. No public machines on either OCF or SCF still use Kerberos passwords.

(3) Expired password. No public machines on either OCF or SCF still use Kerberos passwords.

One-Time Passwords (OTP)

In September, 2001, LC began gradually replacing reusable DCE passwords with more secure "one-time passwords" (OTP) on its open systems.

BACKGROUND.
To comply with DOE Order 205.1, LC is implementing "two-factor" authentication for its open systems (and their passworded services, such as storage and FIS). Two-factor authentication replaces a traditional password reusable for a long period (but vulernable to outside detection during its lifetime) with a series of single-use passwords each comprised of:

- A long-term personal identification number (PIN) concatenated with
- An often-changing string of digits ("token string") generated by a proprietary electronic device (an "authenticator" or "fob" or "token") about the size and shape of a child's eraser.

LC has purchased for every user an authenticator (an RSA SecurID token, with a 4-year lifespan) from RSA Security Inc. and has installed a corresponding (but completely hidden) server that knows which PIN+token strings are valid for each user at any time. At transition time, the LC Hotline provides each user with their own authenticator and a sheet of current instructions for getting a PIN and for activating OTP service at a designated LC web site.

USING ONE-TIME PASSWORDS (OTP).
Your OTP consists of two strings concatenated without a space:

ppppttttt

where

pppp	is your PIN, a 4-(to-8-)digit user-selected string (like the ATM PIN at your bank), which you set or change at this web site (note the 's' in https): https://ratbert.llnl.gov/cgi-bin/pinchg/pinchg
ttttt	is the 6-digit token string currently displayed on your RSA SecurID authenticator. At LC, each token string displays for 30 seconds and can only be used once (but you *can* "save" several for quick sequential use; see below).

Use your OTP just exactly as you would use your former DCE password: there is no extra step(s), no special gateway to visit, and no keying anything on the little authenticator device itself. When you get your authenticator, the LC Hotline provides a current list of LC systems and services that accept OTP (for example, open FIS and OTS do exclusively, and offsite access using VPN or IPA does also).

COUNTDOWN FEATURES.

To help you manage the constantly changing 6-digit token strings (*tttttt*) that appear on the 1-by-3.5-cm display screen of your RSA SecurID authenticator, the screen also displays several countdown features:

At the lower right is a blinking dot (*) that flashes once each second. Along the left edge is a stack of short horizontal bars or hyphens whose size reveals how long the current token string will display:

Number of bars	Time until token changes
5	30 seconds
2	25 seconds
1	15 seconds
0	5 seconds

SAVING TOKEN STRINGS.

You can only use each token string once (concatenated after your PIN) in a password. But the synchronization of each authenticator device with the central security server is loose enough that you *can* use a token string successfully to form a valid password even *after* it has been replaced by another on the authenticator's screen. In fact, the useful life of each (unused, of course) token string in the LC environment is about 90 seconds. A little experimenting will confirm that this long useful life allows you to harvest (write down before it disappears) one token string near the end of its 30-second display period, then record two more during their 30-second displays, and then use those three and the fourth currently on display to log on to as many as four different LC systems or passworded services in quick succession, without waiting 30 seconds between each password use. Saving token strings also lets users who have trouble reading the authenticator screen write down a token string before it disappears and then actually apply it more ergonomically later during its useful life. (The 90-second lifetime does not pose a security problem because as soon as you actually use any token string to construct a valid password, and hence expose it to possible detection, it expires.)

RECOVERY FROM PROBLEMS.

You can give yourself more flexibility in recovering from OTP login problems during remote access if you "enroll" in LC's optional identity-verification service in advance, as described in a later section. (page 28)

ID Verification by Stored Answers

Open LabNet and Livermore Computing jointly offer an optional way for users to verify their identity independently of their passwords by storing in advance answers to preselected questions (sometimes called "questions on file," or more appropriately, "answers on file"). Users who have already stored such answers and who later need to

- reset their OPT PIN when they forget it, or
- unlock their OTP authenticator ("token") when it locks because of too many failed login attempts (especially during remote access)

can perform these functions for themselves at a special web site after they successfully verify their identity by matching their current answers with their previous answers to five questions on an interactive form.

The URL for this (open network) emergency identity-verification service is (note the 's' in https and the uppercase A):

`https://access.llnl.gov/cgi-bin/newAnswer.cgi`

To use this service, follow these steps:

(1) Open the URL above with your web browser. The page that appears (misleadingly called "LLNL Internet Answer Reset Page") offers you a list of 30 possible questions, from which you must select 5. The questions ask about the names of various relatives (youngest aunt on your mother's side, etc.) or places from your past (school locations, etc.).

(2) Click on the check box for each of the 5 questions that you prefer to use for future identity verification.

(3) Click on the SUBMIT button (bottom of the form).

(4) On the page that appears next:
(A) Insert your answer text string for each question into its corresponding text-input box. Note that you can insert *any* string you choose; some cautious users intentionally insert a "secret string" for every answer to decrease the likelihood that an attacker could guess any answer from background knowledge about them.
(B) Click on the SUBMIT button (bottom of this second form).

The web site then returns a "your response has been saved" message to confirm storage of your answers. In the future, if you can repeat these answers to these questions when prompted after an OTP access problem, you can then perform the OTP management or recovery tasks noted above. Or you can call the LC Hotline as usual (use of this service is always optional).

Other Information Sources

SHORT TERM.

Short-term announcements are generally shared either through the "message of the day" (MOTD), which appears on your terminal just after you log in to a specific LC machine, or through NEWS items. A list of unread NEWS items (that is, the file names for unread NEWS postings) appears when you log in. To read a particular item (or, optionally, save it to a local file), use the execute line

```
news newsfile [> myfile ]
```

An archive of old NEWS items is available to web browsers on the open network at https://lc.llnl.gov/computing/news (URL: https://lc.llnl.gov/computing/news) (but your open one-time password is required for access to this secure server).

LONG TERM.

LC provides a variety of user documentation online, including software manuals and user guides that are locally developed to meet LLNL needs, locally adapted documents from other sites, or locally relevant standard publications from vendors. Most LC documentation is now delivered using the World Wide Web (WWW), either directly as HTML files that WWW browsers display or indirectly as (vendor-supplied) PostScript or PDF files that many browsers show by starting suitable slave helper programs (such as GhostView or Adobe Reader). Among the most useful focal points (URLs) for finding or surveying LC-relevant documentation are these:

- "Livermore Computing Documentation," which includes (or links directly to) a subject list of local manuals, an alphabetical list of local manuals, a (reverse) chronological list of LC documentation announcements, and an archive of LC Technical Bulletins.
  OPEN: http://www.llnl.gov/computing (URL: http://www.llnl.gov/computing) [fine-grained topics]
  OPEN: http://www.llnl.gov/LCdocs (URL: http://www.llnl.gov/LCdocs) [whole manuals]
  SCF: http://www.llnl.gov/LCdocs (URL: http://www.llnl.gov/LCdocs)
- "Supported Software and Computing Tools," a tabular guide to the software maintained by LC's Development Environment Group and to the documentation that supports that software.
  OPEN: http://www.llnl.gov/computing/hpc/code/software_tools.html (URL: http://www.llnl.gov/computing/hpc/code/software_tools.html)
  SCF: http://www.llnl.gov/computing/hpc/code/software_tools.html (URL: http://www.llnl.gov/computing/hpc/code/software_tools.html)
- IBM documentation (not product advertising) for ACS machines, served from diverse IBM-maintained sites elsewhere (and hence not available on SCF).
  OPEN: http://www.llnl.gov/LCdocs/ibmdir/ (URL: http://www.llnl.gov/LCdocs/ibmdir/)

PERSONAL PROFILE.

To review your personal "computing profile" on any LC machine, use the locally developed tool called UINFO. UNIFO reports basic background information about you or any other specified user. To run UNIFO type

uinfo [[user] *uname* | [group] *gname* | [bank] *bname*]

where UNIFO tries to guess if its argument is a user name (login name), a group, or a bank, but accepts your disambiguating option if offered as shown here. With no argument at all, UNIFO reports a 5-line help message summarizing its options and ends. With an argument, UNIFO reports as shown below (specific responses may vary from one LC platform to another if you belong to different groups or banks on different machines, for example):

[user] *uname* reports the same information as FINGER about the user whose login name is *uname* (real name, office telephone number, default shell, and home directory) plus the specified user's (numerical) UID, all online (not storage) groups to which the user belongs, and all banks to which the user belongs.

[group] *gname* reports the login name (not real name) of every user who belongs to the specified group *gname*, in alphabetical order. UINFO reports only online groups, not storage groups (see the "Using Storage Groups" section of EZSTORAGE (URL: http://www.llnl.gov/LCdocs/ezstorage)).

[bank] *bname* reports the login name (not real name) of every user who belongs to the specified bank *bname*, in alphabetical order.

Because UNIFO reports on any user (and on groups and banks as well), it is more versatile than the similar LINUX tool USERINFO, which only reports on the user who runs it.

Disclaimer

Keyword Index

To see an alphabetical list of keywords for this document, consult the next section (page 33).

Alphabetical List of Keywords

Keyword	Description
a	The alphabetical index of keywords.
access-administration	Administrative access issues.
access-paths	Three alternative paths compared.
access-techniques	Access-supporting software compared.
availability	Where these programs run.
date	The latest changes to EZACCESS.
dce	DCE password techniques.
entire	This entire document.
file-transfer	Three file-transfer tools.
forms	Fifteen access-support forms.
id-verification	"Answers on file" to confirm identity.
index	The structural index of keywords.
info	Other LC documentation sources.
internet	Open network access (SSH, IPA, VPN).
introduction	Role and goals of EZACCESS.
kerberos	Kerberos password techniques.
login	How to log in with SSH (TELNET blocked).
macx-passwords	Avoiding clear passwords with MacX.
node-names	Numerical node names at LC.
one-time-password	Usage tips for one-time passwords.
otp	Usage tips for one-time passwords.
ots	Terminal-server (dial-up) access.
password-map	Which system uses which passwords.
passwords	Local LC password rules.
path-chart	Paths listed by user status, location.
path-properties	Characteristics of each access path.
revisions	The complete revision history.
scope	Topics covered in EZACCESS.
securenet	Classified network access.
title	The name of this document.
uinfo	Reporting LC personal profiles.
who	Who to contact for assistance.
x-client-authorization	XAUTH client set up tips.
x-server-authorization	XAUTH server set up tips.
x-terminals	Two X-terminal access approaches.

Date and Revisions

Revision Date	Keyword Affected	Description of Change
05Sep06	internet	VPN, IPA inactivity timeout now 30 min.
02Aug06	internet	White references replaced.
	file-transfer	Home dir parallel I/O warning added.
	node-names	White references replaced.
	info	URLs for SCF updated.
10May06	login	Cross ref on X11 forwarding added.
	x-terminals	Cross ref on X11 forwarding added.
18Apr06	introduction	Cross refs reorganized, expanded.
	node-names	Details updated, BG/L added.
18Oct05	securenet	Support URLs updated.
	internet	Support URLs updated. IPA very rarely allowed now. VPN 3000 replaces VPN 5000 client.
13Sep05	internet	Only SSH version-2 protocol now.
	login	Only SSH version-2 protocol now.
16Jun05	internet	IPA scope, time limits restricted.
	node-names	Adelie, Emperor no longer GA.
	passwords	B-453 replaces B-113.
18May05	ots	New URL for new OTS manual.
	node-names	Thunder added.
02Mar05	ots	Post-connect authentication started.
	info	Tools table URLs updated.
01Dec04	node-names	TC2K dropped, UM, Lilac, ALC added.
	internet	12-hour renewable timeout explained.
	login	12-hour timeout noted.
25Aug04	file-transfer	HTAR role expanded.
	node-names	Blue retired.
	info	SCF documentation URL updated.
12Jan04	node-names	ACE (SCF), MCR (OCF) added.
15Sep03	introduction	Cross ref to EZSTORAGE added.
	internet	XSSH role explained.
	login	XSSH role explained.
07Apr03	internet	Two VPN servers now.
	ots	New manual, details updated.
	forms	New OCF URL, more choices.
24Feb03	node-names	Only GPS17-22 are interactive.
	ots	One-time passwords now required.
	otp	Role updated.

03Feb03	node-names	TC retired, GPS grows to 48 nodes.
16Dec02	id-verification	New section on new OTP aid.
	node-names	ILX cluster added.
	index	New keyword for new section.
02Oct02	node-names	Log-on issues elaborated.
	securenet	OAK now SC39, ALDER now SC40.
	login	OAK now SC39, ALDER now SC40.
	passwords	Forest cluster departs.
26Aug02	ots	Many details and URLs updated.
	otp	Scope of OTP use updated.
	info	Several URLs updated.
	file-transfer	SCF anon FTP site deleted.
	forms	SCF forms URL updated.
	dce	SCF password URL updated.
15Jul02	info	UNIFO personal profile tool added.
	uinfo	Keyword added for new tool.
	index	Keyword added for new tool.
15May02	node-names	SCF Linux nodes added.
	internet	OTP optional now for VPN, IPA.
	password-map	SCF Linux nodes added.
	otp	OTS still does not use OTP.
07Feb02	node-names	More nodes, more clusters added.
	path-properties	SCCD becomes ICC in OCF URLs (only).
	x-terminals	GPS replaces Compass cases.
	password-map	More OTP-only cases.
03Oct01	passwords	Section subdivided.
	otp	One-time password section added.
	index	New keyword for new section.
	password-map	Shows where OTP used.
	file-transfer	HTAR role noted.
11Apr01	internet	SSH, IPA, VPN comparison added. Table of access combinations added.
	file-transfer	Cross ref to VPN role added.
08Feb01	internet	All incoming TELNET blocked.
	securenet	SecureNet roles for TELNET, SSH clarified.
	login	All incoming TELNET blocked.
	passwords	No Kerberos passwords remain.
11Dec00	node-names	Linux names changed from lc to lx.
21Nov00	node-names	Linux Cluster names added.
05Oct00	node-names	New section on numerical names.
	index	New keyword for new section.
17Jul00	internet	Globus/Internet job submittal noted.
07Jun00	file-transfer	FIS, anon. FTP details revised.

	passwords	Real words choice suspended.
06Apr00	introduction	Firewall cross reference added.
	internet	Gateway disabled, VPN enabled. SSH role elaborated.
	login	Gateway disabled, SSH elaborated.
	file-transfer	FTP restrictions updated.
	forms	URL for open forms updated.
	passwords	CRAY J90s deleted.
	info	CRAY sources deleted.
20Sep99	macx-passwords	New section on MacX encryption.
	passwords	DCE publicly replaces Kerberos.
	entire	OCF replaces FAST.
02Sep99	file-transfer	DCE passwords for FIS coming.
	passwords	DCE-open password-change web site.
	info	URLs revised, IBM sources added.
	forms	SCF forms URL revised again.
07Jun99	login	SCF TELNET restrictions added.
	passwords	TELNET restrictions on password change. Meiko (Tribble) deleted.
26May99	file-transfer	Firewall effect clarified.
	internet	TELNET blocking scope expanded.
	login	TELNET blocking scope expanded.
29Mar99	file-transfer	Firewall blocks FTP now.
02Feb99	file-transfer	Firewall alert added.
	internet	Firewall effects noted.
	login	Firewall effects on TELNET noted.
11Jan99	file-transfer	SCP added, NFT on open net.
	passwords	SCF Kerberos steps clarified.
	internet	Getting Started URL revised.
22Sep98	forms	SCF forms URL revised.
	passwords	Borg gone, Tera cluster added.
	info	URLs revised.
04May98	securenet	Web-page password restrictions added.
08Apr98	entire	First edition of LC EZACCESS manual.

TRG (05Sep06)